

Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases



News

Thomas Wahl

After several Higher Regional Courts in Germany took the viewpoint that evidence gained from chat messages exchanged between criminals via EncroChat can be used in criminal proceedings in Germany (→ [eucrim 1/2021, 22-23](#)), the Federal Court of Justice (*Bundesgerichtshof*) handed down the first supreme court judgment in these cases ([decision 5 StR 457/21](#)). On 2 March 2022, the Court rejected an appeal on points of law against a conviction by the Regional Court of Hamburg. The Regional Court sentenced the accused to a term of imprisonment of five years for ten crimes of trafficking in narcotics in a not insignificant amount and ordered the confiscation of proceeds of more than €70,000. In some cases, central evidence were text messages sent by the accused via the provider EncroChat to organise drug trafficking. In his appeal, the accused complained, among other things, that this data, obtained from French authorities in 2020 and transmitted to the German authorities, should not have been used as evidence.

Facts of the case

In terms of fact, the Federal Court of Justice (FCJ) stated that the following can be assumed:

In 2017 and 2018, there were indications in France that suspects were carrying out organised drug trafficking via specially encrypted mobile phones ("crypto phones") of the provider EncroChat. With these devices, one could neither make phone calls nor use the internet, but only send chat messages (SMS), create notes or store and send voice messages. Communication was only possible between EncroChat users. Due to a special equipment of the phones and a special encryption technology, law enforcement authorities could neither access the communication conducted with them nor read out the contents of the devices or locate them. The devices were advertised with these features and a guarantee of anonymity. However, they could not be purchased from official sales points, but only from special sellers through anonymous channels at a high price of over €1,600 for a period of use of six months. A legally existing company "EncroChat" could not be found, nor could those responsible for this company or a company headquarters.

The French law enforcement authorities initiated an investigation on suspicion of criminal association, among other things, and found that the encrypted communication between EncroChat users ran via a server operated in Roubaix, France. With authorisation from a French court, they accessed the data on the server. This revealed that over 66,000 SIM cards from a Dutch provider were registered in the system, which were used in a large number of European countries. A decryption of several thousand "notes" from EncroChat

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

Published in
2022, Vol. 17(1) eucrim pp 36 –
37

ISSN: 1862-6947
<https://eucrim.eu>



users proved that they were undoubtedly linked to illegal activities, such as drug trafficking in particular, with up to 60 kg of cocaine.

At the request of the French public prosecutor's office, a court in France authorised the installation of an interception device on the data passing through the French server and stored on the phones as of 1 April 2020. According to initial findings, 63.7% of the phones active in France were certainly used for criminal purposes, the remaining devices (36.3%) were either partly inactive or not yet evaluated. After evaluating the data obtained in the first month, the public prosecutor's office and the court assumed that the EncroChat users were "almost exclusively criminal clientele".

The operation was [assisted by Europol and Eurojust](#). Europol forwarded data to the Federal Criminal Police Office (*Bundeskriminalamt*) since it was found that a large number of serious crimes had been committed by EncroChat users in Germany. The Central Office for Combating Internet Crime at the General Public Prosecutor's Office in Frankfurt am Main then initiated investigations against "unknown persons". In these pre-trial proceedings, a European Investigation Order addressed to France was issued on 2 June 2020 with the request to transfer the EncroChat data concerning Germany and to allow its use in German criminal proceedings. Both were approved by a French court on 13 June 2020.

Criticism

Legal experts voiced concerns over the legality of the operation from a German point of view. They mainly criticised that the secret interception under French law which affected a mass of people without concrete criminal suspicion at that date would not have been possible under German law and severely infringed German fundamental rights of privacy. They also doubted the legality of the way the data were transferred to Germany. This included, among others, the fact that mass data were first exchanged via police channels and the subsequent European Investigation Order served only to rather rubber-stamp these operations without judicial oversight in Germany. In particular, the provisions in [Art. 31 of the Directive on the European Investigation Order](#), which establishes the conditions for the interception of telecommunications for which no technical assistance is needed from the Member State where the subject of the interception is located, were not maintained and this should have consequences on the lawfulness of the use of evidence.

Decision by the Federal Court of Justice

In assessing these legal issues, the [FCJ rejected the arguments](#). It stated that the constitutional legal basis for the use of evidence in criminal proceedings is section 261 of the German Code of Criminal Procedure. The provision establishes the principle of judge's free evaluation of evidence, which also applies to data obtained by way of mutual legal assistance. German law does not contain an explicit provision that such evidence may only be used in a restricted manner. Since the use of data obtained as in this case may involve an encroachment on the secrecy of telecommunications protected by Art. 10 of the Basic Law, the principle of proportionality must be given special constitutional consideration. In this context, the FCJ makes recourse to section 100e, paragraph 6, no. 1 of the Code of Criminal Procedure, which allows the use of personal data "for other purposes" if the collection measure could have been ordered under the conditions of the most intrusive investigative measures of German criminal procedure law – namely an online search or acoustic surveillance of a person's home. This could be done for particularly serious crimes that include the crimes at issue under the Narcotics Act.

Regarding the arguments against the utilisation of evidence asserted by the appeal, the FCJ sees no prohibition.

First, the FCJ reiterates its case law on the use of evidence collected abroad:

- The question of whether such a prohibition exists is exclusively governed by German law;
- A review of the investigative measures (here: the French one) against the standard of foreign law does not take place.

This means that it is therefore not decisive whether a measure carried out in France, as in this case, solely according to French law could also have been ordered in Germany. Furthermore, review of foreign law is not a prerequisite for the transfer of evidence obtained by French authorities under French law to German criminal proceedings. The different prerequisites for ordering in France and Germany can be compensated for at the level of utilisation of evidence in accordance with section 261 of the German Code of Criminal Procedure.

Second, the FCJ found no violation of fundamental values of human rights or European law or of fundamental requirements of the rule of law in the sense of the "ordre public" to be examined in mutual legal assistance, which could lead to a prohibition of the utilisation of evidence. The FCJ stressed above all that, according to the information available to the French authorities after the first access to the data, the investigations did not involve the mass surveillance of a large number of mobile phone users, even without suspicion. Rather, EncroChat presented itself to the French authorities as a network that was designed from the outset to support criminal activities and operated in secret. Based on the initial findings of an almost exclusively criminal use of such phones, a user was therefore already suspicious of criminal activities in the field of organised crime such as drug and arms trafficking or money laundering simply because of the acquisition of an EncroChat mobile phone, which was not available through normal distribution channels and entailed considerable costs.

Third, the FCJ denied that a possible violation by French authorities of the duty to inform Germany in a timely manner about interception measures affecting the territory of the Federal Republic of Germany (Art. 31 of the EIO Directive) can result in a prohibition of the use of evidence. This already results from the subsequent all-round authorisation of the use of the data. Regardless of this, it is questionable whether the duty to notify serves to protect the individual concerned from the use of evidence in Germany. In any case, the necessary weighing of the different interests would lead to a predominance of the state's interest in criminal prosecution. It is also legally unobjectionable that the Public Prosecutor's Office in Frankfurt am Main applied for a comprehensive transfer of evidence in proceedings conducted against unknown persons on the basis of a general suspicion, which ultimately, however, specifically concerned each user.

Lastly, the FCJ sees no hindrances to accept the evidence in view of the exchange of the information prior to the European Investigation Order. In this context, it is pointed out that cross-border transmission of intelligence for criminal prosecution is readily permissible under the European mutual assistance provisions even without a request for mutual assistance. According to the FCJ, a targeted or systematic circumvention of regulations serving the individual legal protection of accused persons by French or German authorities has neither comprehensibly been demonstrated nor been otherwise concretely evident.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).



**Co-funded by
the European Union**